УДК 343.85
DOI https://doi.org/10.32840/1813-338X-2020.3.3.24

О. М. Бодунова
кандидат юридичних наук,
доцент кафедри кримінального права та кримінології
Навчально-наукового інституту права
Університету державної фіскальної служби України

ІСТОРИКО-ПРАВОВІ АСПЕКТИ ВИНИКНЕННЯ КІБЕРЗЛОЧИННОСТІ

Актуальність статті полягає в тому, що сьогодні важко сперечатися щодо питання важливості мережі Інтернет у нашому житті. Інтернет відкриває перспективи для саморозвитку, отримання нових знань, пошуку роботи тощо. Цей ресурс ми використовуємо щодня, навіть свій вільний час можемо проводити на його просторах. Але, пропри це, Інтернет має й іншу сторону, ту, в якій щодня, щогодини вчиняються кримінальні правопорушення, адже платформа забезпечує користувачів повною анонімністю та не обмежує їх у своїх діях. У статті досліджено історію виникнення кіберзлочинності. Зазначено, що дана проблема є чи не найнебезпечнішою у XXI столітті і є нагальна потреба вдосконалення законодавства та проведення роз'яснювальних дій у суспільстві, задля подальшого запобігання створенню нових груп кібершахраїв та розповсюдженню даного явища. Конфлікт в Косово вважається першою Інтернет-війною, в якій групи користувачів комп'ютерної мережі використовували Інтернет для критики бойових дій в Югославії та НАТО, свідомо порушуючи при цьому роботу урядових комп'ютерів, в наслідок чого отримуючи доступ до сайтів, надалі з метою змінити вміст, «дефейс» (deface). Разом з тим у мережі Інтернет поширювалися історії про безпеку і жахи Інтернет-війни, як приклад наводилися різні факти та ідеї громадських діячів, та навіть політиків, саме вони здійснювали пропагандистські дії на надзвичайну кількість користувачів по всьому світі. Усі ці дії дають нам уявлення про те, яким був третій етап розвитку кіберзлочинності. Зроблено висновок, що на сьогодні можна виділити 4 етапи розвитку кіберзлочинності: перший етап – поява такого явища як кіберзлочинність та субкультури хакерів; другий етап – вихід кіберзлочинності на міжнародну арену, поява національних груп хакерів та спеціалізацій кіберзлочинності; третій етап – набуття кіберзлочинністю транснаціонального характеру, поява явища кібертероризму та міжнародних угрупувань хакерів у всіх сферах кіберзлочинності; четвертий етап – використання мережі Інтернет для досягнення політичної мети, поява таких явищ як Інтернет-страйк та Інтернет-війна, а також використання кібератак проти урядів окремих держав.

Ключові слова: *генеза, запобігання, кримінальні правопорушення, законодавство.*

Постановка проблеми. Сьогодні важко сперечатися щодо питання важливості мережі Інтернет у нашому житті. Інтернет відкриває перспективи для саморозвитку, отримання нових знань, пошуку роботи тощо. Цей ресурс ми використовуємо щодня, навіть свій вільний час можемо проводити на його просторах. Але, пропри це, Інтернет має й іншу сторону, ту, в якій щодня, щогодини вчиняються кримінальні правопорушення, адже платформа забезпечує користувачів повною анонімністю та не обмежує їх у своїх діях.

До прикладу, у 2018 році в Україні працівники Департаменту кіберполіції Національної поліції України були залучені до більше ніж одинадцяти тисяч кримінальних проваджень, пов'язаних з кримінальними правопорушеннями у сфері новітніх інформаційних технологій. Протягом року було встановлено, що найбільша кількість протиправних діячів знаходиться в Києві, а також на території Одеської, Миколаївської та Львівської областей [1].

Розвиток та становлення проблеми «кібершахрайства» є новим, тому малодосліджуваним, проте серед вчених, що займалися її вивченням варто виділити В. Голубєва, А. Долгової, К. Касперськи, М. Кастельса, Т. Кесаревої, Л. Куракова, Р. Лемоса, А. Лукацького, І. Рассолова, С. Смірнова. Хоча усі науковці достатньо ґрунтовно розкривають проблему у своїх дослі-

дженнях, необхідно все ж таки узагальнити накопичені знання, зануритися у саму історію виникнення та розвитку кібершахрайства для можливості аналізу дій злочинців відносно розвитку технологій.

Проаналізувавши наукові дослідження та досвід різних країн у боротьбі з даним явищем, можна стверджувати, що дана проблема є чи не найнебезпечнішою у XXI столітті і є нагальна потреба вдосконалення законодавства та проведення роз'яснювальних дій у суспільстві, задля подальшого запобігання створенню нових груп кібершахраїв та розповсюдженню даного явища.

Виклад основного матеріалу. З появою та розвитком всесвітньої мережі Інтернет, неабиякого розвитку набув новий вид злочинності – кіберзлочинність. На сьогодні йому приділяється особлива увага, адже величезний потенціал всесвітнього павутиння може використовуватися у корисливих, нечесних цілях. Кожного дня кіберзлочинці демонструють неймовірну майстерність у виконанні своїх суспільно небезпечних дій, відповідно, це ще більше звертає нашу увагу на актуальність цієї проблеми та закликає до якнайшвидшого пошуку найкращого шляху для її вирішення, який має включати в себе створення відповідних комп'ютерних систем і технологій, з високим рівнем безпеки в мережі та, звичайно, законодавчої бази, яка буде регулювати сповна це питання та встановлювати належні міри покарання за скоєння кримінальних правопорушень даного виду.

Якщо розглядати традиційні види кримінальних правопорушень, такі як вбивство або крадіжка, то кіберзлочинність в порівнянні з ними, явище відносно нове, адже виникло воно саме з появою мережі Інтернет. Слід звернути увагу й на те, що сама по собі мережа Інтернет дає чималі можливості для вчинення кримінальних правопорушень. Основними її рисами є глобальність, анонімність користувачів, охоплення різної за віком та географічним положенням аудиторії, саме вони дозволяють кіберзлочинцям використовувати усі ресурси мережі вправно та уникати покарання за вчинення кримінальних правопорушень.

Становлення та розвиток кіберзлочинності не можна відокремлювати від інформаційної революції, тому початком її відліку доцільно вважати шістдесяті роки минулого століття. Саме у 1962 р. професор Джон Лікрайдер, опублікував свою концепцію розповсюдженої комп'ютерної мережі «Galactic Network» [2, с. 304].

Головним припущенням даної концепції було те, що в майбутньому з'явиться глобальна мережа, приєднатися до якої зможе будь-який охочий, а також у тому, що дана мережа у своїй діяльності може об'єднувати усі комп'ютерні системи світу. Окрім загальної думки вчений детально охарактеризував принципи глобальної мережі, які стали основоположними для мережі Інтернет [3].

Оскільки така ідея та її втілення були новим та надзвичайно цікавим процесом, який міг спростити життя мільйонів людей по всьому світі, то результат не змусив себе чекати. Поява першої мережі комп'ютерів ARPANet (Advanced Research Projects Agency Network), створеної за замовленням Міністерства оборони США. Головна мета даної розробки полягала у тому, щоб створити розподілену систему, яка б не мала чіткого центру, і складалася б з взаємозамінних частин. Спочатку ARPANet мала у складі чотири комп'ютери, розташованих у великих дослідницьких центрах.

Головним завдання мережі була передача інформації та електронне листування, тому жодні серйозні елементи, що обмежували б доступ, в її структурі не існували, оскільки тоді ніхто навіть і не припускав появи злочинців у мережі. Цей недолік надалі успадкує і мережа Інтернет, що в подальшому призведе до явища «анархізм». Непродуманість аспектів безпеки і юридичного контролю при розробці технічних принципів мережі, у майбутньому буде наслідком широкого розповсюдження кіберзлочинності. Далі хотілося б навести кілька фактів, які охарактеризують розвиток кіберзлочинності.

У 1970-х роках з'являються перші комп'ютерні злочинці, яких почали називати «хакерами». Хто ж точно був першим хакером сказати важко, проте у переважній більшості літературних джерел про хакерів та для хакерів, як першого професійного кіберзлочинця згадують Джона Дрейпера, який також проводив першу спеціалізацію хакерів, – фрікери (phreaker), скорочене від телефонний хакер (phone haker). У рядах фрікерів того часу були усім відомі Стів Возняк та Стів Джобс, які в майбутньому стали засновниками «Apple Computers». Саме вони налагодили виробництво пристроїв для злому мереж у домашніх умовах. І цей час доцільно вважати початком розвитку кіберзлочинності [4, с. 296].

У 1983 р. в США, а саме у штаті Мілоукі було проведено перший арешт Інтернет-злочинця, про який відразу повідомили громадськості. Безпосереднім приводом для цього був пер-

ший зареєстрований Інтернет-злом, який був скоєний групою підлітків із шести осіб, які називали себе «група 414» (414 – міжміський телефонний код штату Мілоукі). Ними було зламано 60 комп'ютерів протягом дев'яти днів, серед зламаних були комп'ютери Лос-Аламоської державної лабораторії. Один з членів групи, після проведеного арешту, дав показання і інші її учасники отримали умовний термін відбування покарання [5].

Загалом у 80-х роках прослідковується значне збільшення кількості комп'ютерних атак. Якщо в 1988 р. було тільки шість звернень із даного приводу до центру Інтернет-безпеки CERT, який почав діяти у 1988 р., то в 1989 р. число звернень налічувало 132, а в 1990 – вже 252 [6, с. 118]. Явище кіберзлочинності перестає бути рідкістю, створюються великі групи хакерів, і мережа Інтернет починає ставати простором для незаконної діяльності злочинів. Ці події стають початком другого етапу розвитку кіберзлочинності, для якого характерною є поява нових спеціалізацій Інтернет-злочинців.

У 1984 р. Фред Коен опублікував повідомлення про відкриття перших шкідливих комп'ютерних програм, які здатні до саморозмноження, і визначив їх терміном «комп'ютерний вірус». Також він створив програму, яка ілюструвала спосіб зараження одного комп'ютера іншим [7, с. 320–324].

У 1986 р. в США прийнято перший комп'ютерний закон «The Computer Fraud and Abuse Act» [8], який забороняв незареєстрований доступ до будь-якої комп'ютерної системи. Особливістю даного закону був захист трьох видів несекретної інформації, а саме:

– інформації, що належить фінансовим установам (інформація щодо кредитних карток або ж особистих рахунків);

– інформації, що належить урядовим установам;

– інформації, що належить міжнародним або міжштатним організаціям.

Окрім вищезазначених даних закон також містив статті, зміст яких забороняв пошкодження даних, прикладом цього є розповсюдження вірусів.

Цікаво, що у цьому ж році було заарештовано члена групи "Legion of Doom" Лойда Бланкеншипа, відомого під псевдонімом "The Mentor", який написав знаменитий «Маніфест хакера», – "The Haker Manifesto". Висловлені у даному маніфесті ідеї, навіть до сьогодні вважаються фундаментом хакерської ідеології та культури, а також зазнали чималої популярності в мережі Інтернет. Звичайно, не випадково зростання кількості кіберзлочинів співпало зі зростанням актуальності в комп'ютерному світі ідей хакерів, що є свідченням взаємозв'язку даних явищ.

У 1994 р. світ дізнався про так звану «справу Володимира Льовіна», яку міжнародною кримінальною поліцією було віднесено до категорії «транснаціональний мережевий комп'ютерний злочин». Міжнародна організована злочинна група, що складалася з 12 людей, використовуючи мережу Інтернет та мережу передачі даних «Спрінт/Теленет», подолала захист від незареєстрованого доступу, намагалася здійснити 40 грошових переказів, загальна сума яких становить 10 млн. 700 тис. 952 долари США з особистих рахунків клієнтів банку, які знаходяться в 9 країнах світу, на інші рахунки, зареєстровані у США, Фінляндії, Ізраїлі, Швейцарії, Німеччині, Росії, Нідерландах [8, с. 18]. Це було перше велике міжнародне фінансове кримінальне правопорушення з використанням мережі Інтернет, про яке сповістили громадськість, і яке дало зрозуміти, що кіберзлочини можуть завдавати серйозного фінансового збитку.

У 1998 р. 12-річний хакер зламав комп'ютерну систему, яка координувала водоспуск дамби Теодора Рузвельта в Арізоні. Небезпека його злодіянь полягала у тому, що у разі відкриття зливних воріт дамби вода могла б затопити міста Темп і Месе, загальна чисельність населення яких нараховувала близько 1 млн. жителів. Оцінка даного діяння стала підґрунтям для появи таких термінів як «Інтернет-тероризм», «комп'ютерний тероризм», «кібертероризм». До того ж, це вказало на те, що найбільш уразливою до кібератак є сама мережа Інтернет, адже усі її ключові елементи доступні з будь-якої точки світу.

Поява явища «кібертероризм» і гучні справи про злодіяння міжнародних угрупувань, є свідченням того, що в цей час кіберзлочинність набуває такої ознаки як транснаціональність. Це і стало початком третього етапу у розвитку кіберзлочинності. Небезпечним фактором стало і те, що з розвитком мережі серйозні наслідки могли наступати не тільки у разі умисних кібератак, а й через некомпетентність або ж необережність спеціалістів. Так, у 1997 р. помилка співробітника "Network solutions" стала наслідком того, що сайти, назви яких мали в закінченні ".net" та ".com" стали недоступними. Що свідчить про те, що збій в роботі усієї глобальної мережі стався через неуважність однієї людини.

Також у даний період кібератаки стають способом досягнення політичної мети. Доречно зазначити, що прикладом цього є Інтернет-страйки, при яких усі задіяні особи одночасно заходять на відповідний сайт, приєднуються до відповідного сервісу, відправляють електронні листи, пишуть у форумах із метою обмежити або припинити доступ на сайт іншим користувачам. У наслідок чого відбувається перенавантаження сайту або сервісу, у зв'язку з кількістю надходження запитів, що призводить до збоїв або до повної зупинки роботи ресурсу.

Вперше акцію подібного типу здійснила група, що має назву "Strano Network", яка протестувала проти політики французького уряду щодо питань ядерних програм та й в соціальній сфері. 21.12.1995 дана організована група протягом години здійснювала кібертерористичні дії проти сайтів урядових агентств. При цьому учасники атаки діяли з різних куточків світу за єдиною вказівкою: їм потрібно було за допомогою мережі Інтернет одночасно зайти на урядові сайти, після чого деякі з них дійсно були виведені з робочого стану [9, с. 132–137].

Що далі, тим масштабнішою стає транснаціональність проблеми кіберзлочинності. Таким чином, конфлікт в Косово вважається першою Інтернет-війною, в якій групи користувачів комп'ютерної мережі використовували Інтернет для критики бойових дій в Югославії та НАТО, свідомо порушуючи при цьому роботу урядових комп'ютерів, в наслідок чого отримуючи доступ до сайтів, надалі з метою змінити вміст, «дефейс» (deface). Разом з тим у мережі Інтернет поширювалися історії про безпеку і жахи Інтернет-війни, як приклад наводилися різні факти та ідеї громадських діячів, та навіть політиків, саме вони здійснювали пропагандистські дії на надзвичайну кількість користувачів по всьому світі. Усі ці дії дають нам уявлення про те, яким був третій етап розвитку кіберзлочинності.

Слід згадати, що в даний час практично будь-який політичний або збройний конфлікт йде поряд з організованою протидією у мережі Інтернет. Зокрема, у 2005 р. пройшов ряд кібератак, приводом для яких був шкільний підручник історії, який був виданий в Японії, та у своєму змісті перекручував зміст подій в Китаї в 1930–1940-х рр. XX ст. Якщо детально, то в ньому замовчувалися військові кримінальні правопорушення японських військ під час вторгнення [10]. До списку сайтів, які опинилися під атаками, ввійшли сайти Міністерств, відомств, а також сайти найбільших японських корпорацій та сайти, що були присвячені Другій світовій війні. До того ж, у даній ситуації китайські хакери показали високий рівень майстерності та організованості, що свідчить про надзвичайну синхронність їх атак. Знаючи про те, що у Китаї діє надзвичайний контроль над мережею Інтернет, можна припустити, що дана атака була санкціонована державою. Використання кібератак для досягнення політичних цілей можна вважати початком четвертого етапу в розвитку кіберзлочинності.

Отож, на сьогодні можна виділити 4 етапи розвитку кіберзлочинності.

- Перший етап – поява такого явища як кіберзлочинність та субкультури хакерів.
- Другий етап – вихід кіберзлочинності на міжнародну арену, поява національних груп хакерів та спеціалізацій кіберзлочинності.
- Третій етап – набуття кіберзлочинністю транснаціонального характеру, поява явища кібертероризму та міжнародних угрупувань хакерів у всіх сферах кіберзлочинності.
- Четвертий етап – використання мережі Інтернет для досягнення політичної мети, поява таких явищ як Інтернет-страйк та Інтернет-війна, а також використання кібератак проти урядів окремих держав.

Список використаної літератури:

1. Основні завдання Департаменту кіберполіції Національної поліції України. URL: https://www.cybercrime.gov.ua/contacts.
2. Вехов Б. В. Расследование компьютерных преступлений в странах СНГ : монография / Б. В. Вехов, В. А. Голубев ; под ред. Б. П. Смагоринского. Волгоград : ВА МВД России, 2004. 304 с.
3. Всесвітній огляд економічних злочинів. URL: https://www.pwc.com/ua/uk/Україна.
4. Голубєв В. О. Розслідування комп'ютерних злочинів : монографія / Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. 296 с.
5. Конвенція про кіберзлочинність: міжнародний документ : від 23.11.2001. Сайт Верховної Ради України. URL: http://zakon5.rada.gov.ua/laws/show/994_575.
6. Голубєв В. О. Комп'ютерні злочини в банківській діяльності. З. : Павел, 1997. 118 с.
7. Кравцова М. А. Понятие киберпреступности и ее признаки. *Часопис Київського університету права.* 2015. № 2. С. 320–324.
8. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». *Інформаційна безпека людини, суспільства, держави.* 2010. № 1 (3). С. 18.
9. Пивоваров В. В., Терещенко К. В. Шахрайство її банківськими картками: окремі питання віктимологічної профілактики. *Карпатський приватний часопис.* 2015. С. 132–137.

10. Про ратифікацію Конвенції про кіберзлочинність : Закон України : від 07.09.2005 № 2824-IV. *Сайт Верховної Ради України.* URL: http://zakon2.rada.gov.ua/laws/show/2824-15.

Bodunova O. M. Historical and legal aspects of the emergence of cybercrime

The relevance of the article lies in the fact that today it is difficult to argue about the importance of the Internet in our lives. The Internet opens up prospects for self-development, gaining new knowledge, finding a job, etc. We use this resource every day, we can even spend our free time on its spaces. But, despite this, the Internet has another side, the one in which criminal offenses are committed every day, every hour, because the platform provides users with complete anonymity and does not limit their actions. The article examines the history of cybercrime. It is noted that this problem is almost the most dangerous in the 21st century and there is an urgent need to improve the legislation and carry out explanatory actions in society, in order to further prevent the creation of new groups of cyber fraudsters and the spread of this phenomenon. The conflict in Kosovo is considered the first Internet war, in which groups of computer users used the Internet to criticize the fighting in Yugoslavia and NATO, while deliberately disrupting the operation of government computers, thereby gaining access to sites, later with the aim of changing content, "deface" (deface). At the same time, stories about the safety and horrors of the Internet war spread on the Internet, as an example various facts and ideas of public figures and even politicians were cited, they were the ones who carried out propaganda actions on an extraordinary number of users around the world. All these actions give us an idea of what was the third stage of the development of cybercrime. It was concluded that today it is possible to distinguish 4 stages of the development of cybercrime: the first stage is the emergence of such a phenomenon as cybercrime and hacker subcultures; the second stage is the entry of cybercrime into the international arena, the emergence of national groups of hackers and specializations of cybercrime; the third stage – the acquisition of transnational character by cybercrime, the emergence of the phenomenon of cyberterrorism and international groups of hackers in all spheres of cybercrime; the fourth stage is the use of the Internet to achieve a political goal, the emergence of such phenomena as the Internet strike and Internet war, as well as the use of cyber attacks against the governments of individual states.

Key words: *genesis, prevention, criminal offenses, legislation.*